

Prevention of spoofing in telecommunications systems

Patent number: JP2003518821T

Publication date: 2003-06-10

Inventor:

Applicant:

Classification:

- international: **H04L12/56; H04L29/06;
H04L29/08; H04L29/12;
H04Q7/22; H04L12/56;
H04L29/06; H04L29/08;
H04L29/12; H04Q7/22; (IPC1-7);
H04L12/56; H04Q7/38**

- european: **H04L29/06C6G; H04L12/56B;
H04L29/06J1; H04L29/08A7W;
H04L29/12A**

Application number: JP20010547792T 20001219

Priority number(s): FI19990002767 19991222;
WO2000FI01114 20001219

Also published as:

■ WO0147179 (A1)
■ US2002181448 (A1)
■ FI110975B (B)

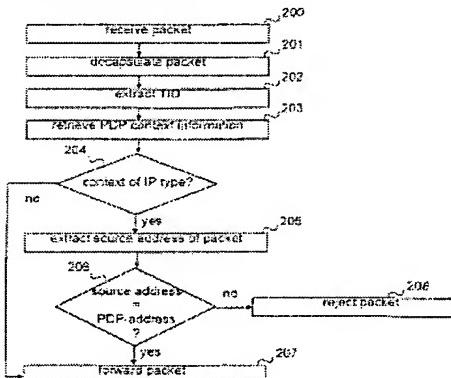
Report a data error here

Abstract not available for JP2003518821T

Abstract of corresponding document: **US2002181448**

In a packet radio network a packet data address is activated for a terminal for transmitting data packets between the terminal and an external network. Information on the activated packet data address is stored at least in the edge nodes of the network. To prevent spoofing, i.e.

misrepresentation of sender data, the method and network node of the invention comprise checking (206) in the node whether the source address of the packet transmitted from the terminal is the same as the packet data address used in the transmission of the packet or does the source address belong to a set of allowed packet data addresses. The packet is transmitted (207) from the node towards the destination address only if the addresses are identical or the source address belongs to the set of allowed packet data addresses.



Data supplied from the **esp@cenet** database - Worldwide

特表2003-518821

(P2003-518821A)

(43) 公表日 平成15年6月10日(2003.6.10)

(51) Int. C1.⁷
 H 04 L 12/56
 H 04 Q 7/38

識別記号
 1 0 0

F I
 H 04 L 12/56 1 0 0 Z 5K030
 H 04 B 7/26 1 0 9 R 5K067

マークト(参考)

審査請求 有 予備審査請求 有 (全26頁)

(21) 出願番号 特願2001-547792(P2001-547792)
 (86) (22) 出願日 平成12年12月19日(2000.12.19)
 (85) 翻訳文提出日 平成14年6月20日(2002.6.20)
 (86) 國際出願番号 PCT/FI00/01114
 (87) 國際公開番号 WO01/047179
 (87) 國際公開日 平成13年6月28日(2001.6.28)
 (31) 優先権主張番号 19992767
 (32) 優先日 平成11年12月22日(1999.12.22)
 (33) 優先権主張国 フィンランド(F I)

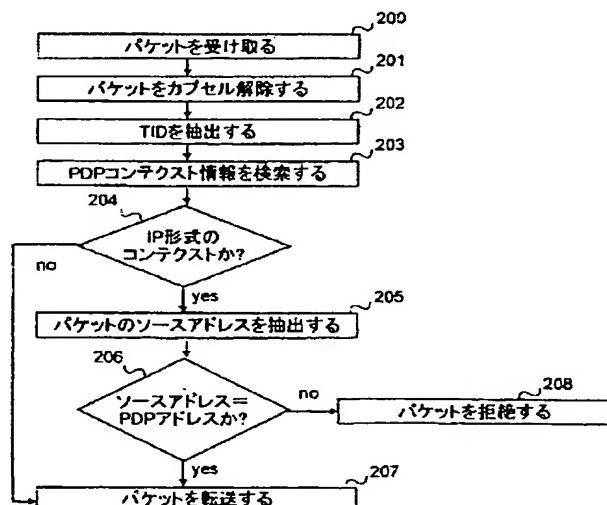
(71) 出願人 ノキア コーポレイション
 フィンランド エフィーエン-02150 エ
 スブー ケイララーデンティエ 4
 (72) 発明者 ウスケラ サミ
 フィンランド エフィーエン-00530 ヘ
 ルシンキ シルタサーレンカトウ 26 ア
 -1
 (72) 発明者 ヨキネン ハンヌ テー
 フィンランド エフィーエン-03300 オ
 タランピ ヨキペロンティエ 375 アー
 (74) 代理人 弁理士 中村 稔(外9名)

最終頁に続く

(54) 【発明の名称】 テレコミュニケーションシステムにおけるなりすましの防止

(57) 【要約】

パケット無線ネットワークにおいて、ターミナルに対するパケットデータアドレスがアクチベートされて、ターミナルと外部ネットワークとの間にデータパケットを送信する。アクチベートされたパケットデータアドレスに関する情報は、少なくとも、ネットワークのエッジノードに記憶される。なりすまし即ち送信者データの偽った表示を防止するため、本発明の方法及びネットワークノードは、ターミナルから送信されたパケットのソースアドレスが、パケットの送信に使用されたパケットデータアドレスと同じであるかどうか、又はそのソースアドレスが許容パケットデータアドレスのリストに属するかどうかを上記ノードにおいてチェックする(206)ことを含む。上記両アドレスが同じであるか又はソースアドレスが許容パケットデータアドレスのリストに属する場合のみ、パケットは、ノードから行先アドレスに向けて送信される(207)。



【特許請求の範囲】

【請求項1】 データパケットを送信することのできるターミナルと、第1サブシステム内でデータパケットを受信して転送するための少なくとも1つのノードとを備えたテレコミュニケーションシステムにおいてなりすましを防止するための方法であって、上記第1サブシステム内でターミナルに対するパケットデータアドレスをアクチベートしてターミナルと第2サブシステムとの間にデータパケットを送信し、パケットデータアドレスのデータパケットをルーティングする際に通る第1サブシステムの少なくとも1つのノードにパケットデータアドレスを記憶し、そしてターミナルから送信されたパケットを上記ノードで受け取り、パケットは、行先アドレス及びソースアドレスを含むものであるような方法において、

パケットのソースアドレスがパケットデータアドレスと同じであるかどうかを上記ノードにおいてチェックし(206)、そして

上記両アドレスが同じである場合にのみノードから行先アドレスに向けてパケットを送信する(207)、

という段階を備えたことを特徴とする方法。

【請求項2】 データパケットを送信することのできるターミナルと、第1サブシステム内でデータパケットを受信して転送するための少なくとも1つのノードとを備えたテレコミュニケーションシステムにおいてなりすましを防止するための方法であって、上記第1サブシステム内でターミナルに対するパケットデータアドレスをアクチベートしてターミナルと第2サブシステムとの間にデータパケットを送信し、パケットデータアドレスのデータパケットをルーティングする際に通る第1サブシステムの少なくとも1つのノードにパケットデータアドレスを記憶し、そしてターミナルから送信されたパケットを上記ノードで受け取り、パケットは、行先アドレス及びソースアドレスを含むものであるような方法において、

パケットデータアドレスを1組の許容パケットデータアドレスとして定義し、パケットのソースアドレスが上記1組の許容パケットデータアドレスに属するかどうか上記ノードにおいてチェックし(206)、そして

パケットのソースアドレスが上記1組の許容パケットデータアドレスに属する場合にのみノードから行先アドレスに向けてパケットを送信する(207)、という段階を備えたことを特徴とする方法。

【請求項3】 上記ノードは、ターミナルから第2サブシステムへデータパケットをルーティングする第1サブシステムのゲートウェイサポートノードである請求項1又は2に記載の方法。

【請求項4】 上記ノードは、移動ステーションにサービスするサポートノードであって、ターミナルから受け取ったパケットを第1サブシステムに向けてルーティングするサポートノードである請求項1又は2に記載の方法。

【請求項5】 上記第1サブシステムは、GTPプロトコルを使用するパケット無線ネットワークであり、そして上記パケットデータアドレスは、それに対応するPDPコンテキストをアクチベートすることによりアクチベートされる請求項1ないし4のいずれかに記載の方法。

【請求項6】 上記方法は、更に、

第1パケットデータアドレスの形式に関する情報を上記ノードに維持し、この情報は、上記チェックが行われるところの少なくとも1つのパケットデータアドレス形式を含み、そして

パケットデータアドレスが第1パケットデータアドレス形式である場合にのみ上記チェックを実行する、

という段階を備えた請求項1ないし5のいずれかに記載の方法。

【請求項7】 上記第1パケットデータアドレス形式は、インターネットプロトコルに基づく少なくともIPアドレスを含む請求項6に記載の方法。

【請求項8】 パケットネットワークのターミナル(MS)から受信器(2, 4)へデータパケットを送信するためのパケットネットワークのネットワークノード(SGSN, GGSN)であって、ターミナルがデータパケットを送信するときに使用できるターミナルの少なくとも1つのパケットデータアドレスをアクチベートし、そしてターミナルから受け取ったパケットを、ターミナルにより使用されるパケットデータアドレスにアタッチするよう構成されたネットワークノード(SGSN, GGSN)において、

パケットを受信するのに応答して、パケットのソースアドレスを、ターミナルにより使用されるパケットデータアドレスと比較し、そして両アドレスが同一である場合にのみ、ネットワークノードからパケットの行先アドレスに向けてパケットを送信するように構成されたことを特徴とするネットワークノード(SGSN, GGSN)。

【請求項9】 パケットネットワークのターミナル(MS)から受信器(2, 4)へデータパケットを送信するためのパケットネットワークのネットワークノード(SGSN, GGSN)であって、ターミナルがデータパケットを送信するときに使用できるターミナルの少なくとも1つのパケットデータアドレスをアチャバートし、そしてターミナルから受け取ったパケットを、ターミナルにより使用されるパケットデータアドレスにアタッチするよう構成されたネットワークノード(SGSN, GGSN)において、

上記パケットデータアドレスは、1組の許容パケットデータアドレスとして定義され、

パケットを受信するのに応答して、ネットワークノード(SGSN, GGSN)は、パケットのソースアドレスが、ターミナルにより使用されるパケットデータアドレスの上記1組の許容パケットデータアドレスに属するかどうかチェックし、そしてそのソースアドレスが上記1組の許容パケットデータアドレスに属する場合にのみネットワークノードからパケットの行先アドレスに向けてパケットを送信するように構成されたことを特徴とするネットワークノード(SGSN, GGSN)。

【請求項10】 上記ネットワークノード(SGSN, GGSN)は、上記比較が実行されるところの第1パケットデータアドレス形式に関する情報を維持し、そしてターミナルにより使用されるパケットデータアドレスが第1パケットデータアドレス形式である場合にのみ比較を実行するよう構成された請求項8又は9に記載のネットワークノード。

【請求項11】 上記ネットワークノードは、GTPプロトコルを使用するパケット無線ネットワーク(GPRS)のゲートウェイサポートノード(GGSN)である請求項8、9又は10に記載のネットワークノード。

【請求項12】 上記ネットワークノードは、GTPプロトコルを使用する

パケット無線ネットワーク(GPRS)においてターミナルにサービスするサポートノード(SGSN)である請求項8、9又は10に記載のネットワークノード。

【発明の詳細な説明】**【0001】****【技術分野】**

本発明は、パケットデータを送信することのできるテレコミュニケーションシステムにおけるなりすましの防止に係る。より詳細には、本発明は、移動通信システムにおいて移動ステーションから送信されたIP（インターネットプロトコル）パケットにおける送信者データのなりすましを防止することに係る。

【0002】**【背景技術】**

移動通信ネットワークは、移動データの送信用に実際のデータネットワークへのアクセスをユーザに与える有効なアクセスネットワークとして機能する。移動データ送信は、パン・ヨーロピアン移動通信システムGSM（移動通信用のグローバルシステム）のようなデジタル移動通信システムによって特に良好にサポートされる。本明細書において、「データ」という語は、デジタルテレコミュニケーションシステムにおいて送信されるいかなる情報も指す。このような情報は、デジタルエンコードされた音声及び／又は映像、コンピュータ間データトライック、テレファックスデータ、又はプログラムコードのショートセクション等を含む。移動通信システムとは、一般に、ユーザがシステムのサービスエリア内を移動するときにワイヤレス通信を使用するいかなるテレコミュニケーションシステムも指す。移動通信システムの典型的な例は、公衆地上移動ネットワークPLMNである。移動通信ネットワークは、外部ネットワーク、ホスト、又は特定のサービス手順により提供されるサービスへのワイヤレスアクセスをユーザに与えるアクセスネットワークであることがほとんどである。

【0003】

移動通信システムを開発する主たる目標の1つは、移動ステーションがホストとしても機能し得るように移動通信ネットワークを経てIPサービスを利用する機会を提供することである。これは、例えば、汎用パケット無線サービスGPRSにおいて考えられる。GPRSサービスは、GSMシステムにおいて移動データターミナルと外部データネットワークとの間にパケットデータ送信を与える。

GPRSデータを送信及び受信するために、移動ステーションは、PDP（パケットデータプロトコル）アクチベーション手順を要求することによりそれが使用を望むパケットデータアドレスをアクチベートしなければならない。このオペレーションは、移動ステーションを対応するゲートウェイサポートノードに知らしめ、従って、アクチベートされたパケットデータアドレスを使用して外部データネットワークとのインターワーキングを開始することができる。UMTS（ユニバーサル移動通信システム）及びIMT-2000（国際移動テレコミュニケーション2000）のような「第3世代移動通信システム」に対しても同様の解決策が構成されている。

【0004】

特に、IPネットワークでは、IPデータパケットのソースアドレスのなりすまし即ち偽造が容易である。換言すれば、IPパケットを送信するホストは、他の誰かであると偽り、そしてAの名前でBへパケットを送信し、Bは、Aに応答を送信する。この場合に、A及びBの両方が互いに妨害する。この問題に対する1つの解決策は、ファイアウォールを使用することである。しかしながら、この解決策において、ユーザは認証されず、ソース及び行先アドレスのみが監視される。ファイアウォールでは、ソースアドレスが、通常、サブネットワークの精度で記述される。その結果、ファイアウォールは、パケットの真の送信者を知ることができず、同じサブネットワークのホストがそれら自体を互いに代表することができる。ファイアウォールに許されたソースアドレスを前もって知らねばならず、そして移動ステーションは、そのIPアドレスを変更せずに1つのファイアウォールのエリアから別のファイアウォールのエリアへ移動できねばならないので、ファイアウォールの許容ソースアドレスは、実際には、ファイアウォールによって保護されるサブネットワークにアクセスできる全ての移動ステーションをカバーする。これにより生じる問題は、IPパケットのソースアドレスが信頼できるものでなく、なりすましを防止するために、移動ホストを別々に認証しなければならないことである。なりすましの防止は、ホストが課金されるIPサービスが利用されるときに特に重要である。しかしながら、信頼性の高い認証手順は、ネットワークの遅延を増加するか、或いは移動通信ネットワークの限定された

リソース即ちエインターフェイスを浪費することになる。

【0005】

【発明の開示】

本発明の目的は、データパケットの受信者が、データパケットのソースアドレスがパケットの真の送信者を示している事実を信頼できるようにする方法、及びこの方法を実施する装置を提供することである。

本発明のこの目的は、データパケットを送信することのできるターミナルと、第1サブシステム内でデータパケットを受信して転送するための少なくとも1つのノードとを備えたテレコミュニケーションシステムにおいてなりすましを防止するための方法により達成される。この方法は、上記第1サブシステム内でターミナルに対するパケットデータアドレスをアクチベートしてターミナルと第2サブシステムとの間にデータパケットを送信し、パケットデータアドレスのデータパケットをルーティングする際に通る第1サブシステムの少なくとも1つのノードにパケットデータアドレスを記憶し、そしてターミナルから送信されたパケットを上記ノードで受け取り、パケットは、行先アドレス及びソースアドレスを含むものであり、更に、パケットのソースアドレスがパケットデータアドレスと同じであるかどうかを上記ノードにおいてチェックし、そして両アドレスが同じである場合にのみノードから行先アドレスに向けてパケットを送信するという段階を備えている。

【0006】

更に、本発明は、データパケットを送信することのできるターミナルと、第1サブシステム内でデータパケットを受信して転送するための少なくとも1つのノードとを備えたテレコミュニケーションシステムにおいてなりすましを防止するための方法であって、上記第1サブシステム内でターミナルに対するパケットデータアドレスをアクチベートしてターミナルと第2サブシステムとの間にデータパケットを送信し、パケットデータアドレスのデータパケットをルーティングする際に通る第1サブシステムの少なくとも1つのノードにパケットデータアドレスを記憶し、ターミナルから送信されたパケットを上記ノードで受け取り、パケットは、行先アドレス及びソースアドレスを含むものであり、更に、パケットデ

一タアドレスを1組の許容パケットデータアドレスとして定義し、パケットのソースアドレスが上記1組の許容パケットデータアドレスに属するかどうか上記ノードにおいてチェックし、そしてパケットのソースアドレスが上記1組の許容パケットデータアドレスに属する場合にのみノードから行先アドレスに向けてパケットを送信するという段階を備えた方法にも係る。

【0007】

又、本発明は、パケットネットワークのターミナルから受信器へデータパケットを送信するためのパケットネットワークのネットワークノードであって、ターミナルがデータパケットを送信するときに使用できるターミナルの少なくとも1つのパケットデータアドレスをアクチベートし、そしてターミナルから受け取ったパケットを、ターミナルにより使用されるパケットデータアドレスにアタッチするよう構成されたネットワークノードにも係る。このネットワークノードは、パケットを受信するのに応答して、パケットのソースアドレスを、ターミナルにより使用されるパケットデータアドレスと比較し、そして両アドレスが同一である場合にのみ、ネットワークノードからパケットの行先アドレスに向けてパケットを送信するように構成されたことを特徴とする。

【0008】

更に、本発明は、パケットネットワークのターミナルから受信器へデータパケットを送信するためのパケットネットワークのネットワークノードであって、ターミナルがデータパケットを送信するときに使用できるターミナルの少なくとも1つのパケットデータアドレスをアクチベートし、そしてターミナルから受け取ったパケットを、ターミナルにより使用されるパケットデータアドレスにアタッチするよう構成されたネットワークノードにも係る。このネットワークノードは、パケットデータアドレスが1組の許容パケットデータアドレスとして定義され、パケットを受信するのに応答して、ネットワークノードが、パケットのソースアドレスが、ターミナルにより使用されるパケットデータアドレスの上記1組の許容パケットデータアドレスに属するかどうかチェックし、そしてそのソースアドレスが上記1組の許容パケットデータアドレスに属する場合にのみネットワークノードからパケットの行先アドレスに向けてパケットを送信するように構成

されたことを特徴とする。

【0009】

本発明は、データパケットを送信するためにアクチベートされたパケットデータアドレスにより、例えば、ゲートウェイサポートノードGGSNは、データパケットを送信した移動ステーションのパケットデータアドレスを知るという考え方をベースとする。従って、ゲートウェイサポートノードGGSNは、データパケットのソースアドレスを、移動ステーションにより使用されるパケットデータアドレスと比較するだけでよい。両アドレスが同一である場合には、アドレスが偽造されたものではなく、パケットは、行先アドレスへ転送することができる。

本発明の効果は、実施が非常に簡単で、しかも、なりすましを防止できることである。例えば、IPパケットの受信者は、IPパケットのソースアドレスがIPパケットの送信者を認証するということを信頼することができる。付加的な認証メカニズムは必要とされず、従って、ネットワークに負荷がかからず、遅延を最小にすることができます。又、本発明は、課金可能なサービスの実施を容易にする。というのは、サービス創作者は、データパケットのソースアドレスが、課金されるべきユーザを指示することを信頼できるからである。

【0010】

本発明の好ましい実施形態では、ゲートウェイサポートノードにおいて比較が行われる。この実施形態の効果は、ネットワーク内で数の少ない要素に比較メカニズムが追加されることである。

本発明の別の好ましい実施形態では、移動ステーションにサービスするパケット無線ネットワークのエッジノードにおいて比較が行われる。この実施形態の効果は、いずれにせよ供給されないパケットを送信することによりパケット無線ネットワークに負荷がかからないことである。

本発明の好ましい実施形態では、ソースアドレスのなりすまし即ち偽造を可能にするパケットデータプロトコルを使用するパケットに対してのみ比較が実行される。この実施形態の効果は、ソースアドレスを偽造できないパケットについては無益に比較が行われないことである。

本発明の方法及びネットワークノードの好ましい実施形態は、従属請求項に記

載する。

【0011】

【発明を実施するための最良の形態】

以下、添付図面を参照して、本発明の好ましい実施形態を詳細に説明する。

本発明は、個々のパケットデータアドレスが、GPRSシステムの場合のように、使用の前にアクチベートされ、そしてそのネットワークインフラストラクチャーにおいて情報がユーザのアクティブパケットデータアドレスに維持されるようないかなるパケット交換システムにも適用できる。これらのシステムは、「第3世代の移動通信システム」、例えば、ユニバーサル移動テレコミュニケーションシステム(UMTS)及びIMT-2000(国際移動テレコミュニケーション)や、GSMシステムに対応する移動通信システム、例えば、DCS1800(188MHz用のデジタルセルラーシステム及びPCS(パーソナル通信システム)や、上記システムをベースとしそしてGPRS型のパケット無線を実施するWLLシステムを含む。更に、本発明は、移動通信システム以外のシステム、例えば、ケーブルモdemネットワーク及び同様の固定システムにも適用することができる。本発明は、以下、GSMシステムのGPRSサービスを一例として使用して説明するが、このようなシステムに限定されるものではない。移動通信システムの定義は、急速に変化し、本発明に対して付加的な変更が必要となるであろう。このため、全ての用語及び表現は、広く解釈されるべきであり、それらは本発明を単に例示するものであって何らそれに限定されるものではないことを銘記されたい。

【0012】

図1は、GPRSサービスのネットワークアーキテクチャーを一般的なレベルで示す。というのは、ネットワークの詳細な構造は本発明に関与しないからである。GSMシステムの構造及び機能は、当業者にとって非常に馴染み深いものである。GPRSサービスの構造は、例えば、参考としてここに取り上げるETS I仕様書03.60、バージョン6.0.0(デジタルセルラーテレコミュニケーションズシステム(フェーズ2+)；汎用パケット無線サービス(GPRS)；サービス説明；段階2)に定義されている。GPRSサービスは、無線アクセ

スを与えるアクセスネットワークを含み、これは、図1においてGSMシステムのベースステーションサブシステムBSSにより表わされる。又、GPRSサービスは、パケットデータネットワークPDNと移動ステーションMSとの間のデータのパケット交換送信に対してGPRSサービスのサポートノードをエッジノードとして備えている。サポートノードは、サービングGPRSサポートノードSGSN及びゲートウェイGPRSサポートノードGGSNを含む。これらのサポートノードSGSN及びGGSNは、バックボーンネットワーク1により相互接続される。SGSN及びGGSNの機能は、同じネットワークノードに物理的に結合することができ、この場合に、オペレータのバックボーンネットワークは不必要であることに注意されたい。しかしながら、論理的には、ノードは個別のノードである。

【0013】

サービングGPRSサポートノードSGSNは、移動ステーションMSにサービスする。各サポートノードSGSNは、セルラーパケット無線ネットワークの1つ以上のセルのエリア内で移動データターミナル即ち移動ステーションMSに対してパケットデータサービスを生成する。このため、各サポートノードSGSNは、典型的に、GSM移動通信システム（典型的にベースステーションサブシステムBSSのベースステーションコントローラ）に接続され、中間の移動通信ネットワークがSGSNと移動ステーションとの間に無線アクセス及びパケット交換データ送信を与えるようにされる。換言すれば、セル内の移動ステーションMSは、無線インターフェイスを経てベースステーションと通信し、そして更にベースステーションサブシステムを経て、セルがサービスエリアに属するところのサポートノードSGSNと通信する。SGSNノードの主たるファンクションは、そのサービスエリアにおいて新たなGPRS移動ステーションを検出し、新たな移動ステーションMSのGPRSレジスターへの登録を実行し、データパケットをGPRS移動ステーションへ送信し又はそこから受信し、そしてそのサービスエリア内の移動ステーションMSの位置についてファイルを維持することである。これは、SGSNが、認証及び暗号化手順のようなセキュリティ機能及びアクセス制御を実行することを意味する。独特のトンネルを使用して、SGSNは

、移動ステーションから受け取ったパケットをカプセル化形態でGPRSバックボーンネットワークを経てGGSNノードへルーティングし、そこで、パケットデータアドレスがアクチベートされる。

【0014】

GPRSゲートウェイサポートノードGGSNは、オペレータのGPRSネットワークを外部システム、データネットワーク、例えば、IPネットワーク（インターネット）又はX.25ネットワーク、及びサーバー2に接続する。又、GGSNは、個人会社のネットワーク又はホストに直接接続することもできる。図1の例では、GGSNは、信頼性のあるIPネットワーク3を経てサーバー2に接続され、そしてファイアウォールFWを経てインターネット4に接続される。GGSNは、GPRS加入者のPDPアドレス及びルーティング情報、即ちSGSNアドレスを含む。GGSNは、移動ステーションMSのルートに関してSGSNノードによって発生されるルート情報を使用して位置ファイルを更新する。GGSNは、外部アドレスと内部のルーティング情報（例えば、SGSN）との間のルーターとして機能する。換言すれば、GGSNは、外部データネットワークのプロトコルパケットをカプセル化形態でGPRSバックボーンネットワークを経てSGSNノードへルーティングし、該SGSNノードは、所与の時間に、移動ステーションMSにサービスする。又、これは、移動ステーションから送信されたパケットをカプセル解除し、そして外部データネットワークのパケットを関連データネットワークに送信する。又、GGSNは、ある移動ステーションからネットワーク内の別の移動ステーションへパケットを送信する。更に、GGSNは、データトラフィックの勘定についても役割を果たす。

【0015】

移動ステーションMSは、パケットデータ送信をサポートしそしてネットワークへの無線インターフェイスを有するいかなる移動ノードでもよい。例えば、パケット無線オペレーションを行うことのできるセルラー電話に接続されたラップトップPC、或いは小型コンピュータ及びパケット無線電話の一体化された組み合わせであってもよい。移動ステーションMSの他の実施形態は、種々のページャー、リモートコントローラ、監視及び／又はデータ収集装置、等を含む。又、

移動ステーションは、移動ノード又は移動ホストとも称される。

【0016】

GPRSサービスにアクセスするために、移動ステーションは、先ず、GPRSアタッチオペレーションを実行することによりその存在をネットワークに知らしめねばならない。このオペレーションは、移動ステーションMSとSGSNノードとの間に論理的リンクを確立し、そして移動ステーションをGPRSを経てショートメッセージに使用できるようにするか、或いは同様のメッセージを接続なしに送信させ、SGSNを経てページングを行いそして到来するGPRSデータを通知するようにさせる。より正確さを期すために、移動ステーションMSがGPRSネットワークにアタッチするときに（GPRSアタッチ手順において）、SGSNは、移動管理コンテクスト（MMコンテクスト）を形成し、そしてプロトコル層において移動ステーションMSとSGSNノードとの間に論理リンクL LC（論理リンク制御）が確立される。MMコンテクストは、SGSNノード及び移動ステーションMSに記憶される。SGSNノードのMMコンテクストは、加入者のIMSI、TLLI（一時的論理リンク識別子）、位置及びルーティング情報等の加入者データを含む。

【0017】

GPRSデータを送信及び受信するために、移動ステーションMSは、PDPアクチベーション手順を要求することにより、PDPアドレス、即ちそれが使用を望むパケットデータアドレスをアクチベートしなければならない。PDPコンテクストは、移動ステーションがGPRSネットワークにアタッチするときにアクチベートすることができる。或いは又、移動ステーションは、PDPコンテクストを後でアクチベートしてもよいし、又はGPRSネットワークから受け取られたアクチベーション要求の結果としてアクチベーションが実行されてもよい（GPRSネットワーク要求PDPコンテクストアクチベーション）。GPRSインターフェイスは、パケットデータアドレス及びそれに関連したパラメータを記述する1つ以上の個々のPDPコンテクストを含む。より詳細には、PDPコンテクストは、PDP形式（例えば、X.25又はIP）、PDPアドレス（例えば、IPアドレス）、サービスクオリティQoS及びNSAPI（ネットワーク

サービスアクセスポイント識別子) のような種々のデータ送信パラメータを定義する。1つの移動ステーションは、多数の同様のPDPアドレス、例えば、異なるIPアドレスをPDPアドレスとしてもつことができる(即ち、移動ステーションは、多数のIP型コンテクストを有する)。例えば、IPプロトコルを使用して送信される種々のクオリティ及び価格のサービスに対して種々のIPアドレス即ちコンテクストを使用することができる。PDPコンテクストのパケットデータアドレスは、永久的(即ちホーム位置レジスタの加入者データにおいて定義される)であるか、又は動的であり、この場合は、GGSNがPDPアクチベーション手順の間にパケットデータアドレスを割り当てる。PDPアクチベーション手順は、PDPコンテクストをアクチベートし、そして移動ステーションを対応するGGSNノードに知らしめ、その結果、外部データネットワークとのインターワーキングを開始させる。PDPコンテクストアクチベーションの間に、PDPコンテクストが移動ステーション並びにGGSN及びSGSNノードに生成される。PDPコンテクストがアクチベートされると、ユーザがGSM手順により認証され、従って、PDPコンテクストアクチベーションにおいてターミナルに与えられるパケットデータアドレス、例えば、IPアドレスを、ユーザの認識コード、例えば、IMSI(国際移動加入者認識)に確実にアタッチすることができる。

【0018】

PDPコンテクストが生成され、そしてGTPプロトコル(GPRSトンネリングプロトコル)を用いてパケットがトンネル送信される。移動ステーションMSは、PDPコンテクストを特定のメッセージ「アクチベートPDPコンテクスト要求」でアクチベートし、この場合、移動ステーションは、TLLI、PDP形式、要求されたQoS及びNSAPIに関する情報、及び任意であるがPDPアドレス及びアクセスポイント名APNに関する情報を与える。SGSNは、「クリエートPDPコンテクスト」メッセージをGGSNノードに送信し、該ノードは、PDPコンテクストを生成して、それをSGSNノードに送信する。「アクチベートPDPコンテクスト要求」メッセージ(及び「クリエートPDPコンテクスト」メッセージ)がPDPアドレスを含まない場合には、GGSNは、P

PDPコンテクストの生成中にPDPアドレスを割り当て、そしてSGSNへ送信されるべきPDPコンテクストに動的なPDPアドレスを含む。SGSNは、PDPコンテクストを「アクチベートPDPコンテクスト応答」メッセージにおいて移動ステーションMSへ送信する。PDPコンテクストは、移動ステーションMS、SGSNノード及びGGSNノードに記憶される。サービングSGSNノードでは、各PDPコンテクストがMMコンテクストと共に記憶される。MSが新たなSGSNノードのエリアへローミングするときには、新たなSGSNが古いSGSNノードからMMコンテクスト及びPDPコンテクストを要求する。

【0019】

従って、PDPコンテクストアクチベーション手順では、移動ステーションMSとGGSNノードとの間に仮想接続又はリンクが確立される。同時に、このPDPコンテクスト及びパケットデータアドレスに対してGGSNとSGSNとの間に独特的のトンネルが形成される。トンネルは、IPパケットがたどるルートであり、これにより、移動ステーションから送信されたパケットは、GGSNにおいてあるPDPコンテクスト及びあるパケットデータアドレスにアタッチされる。換言すれば、トンネルは、パケットを送信するときに使用される移動ステーションのパケットデータアドレスを識別するのに使用される。パケットは、TID（トンネル識別子）と共に、又はGTPプロトコルが使用されるときにはトンネルエンドポイント識別子と共に、あるPDPコンテクストにアタッチされる。TIDは、NSAPI及びIMSIを含む。PDPコンテクストアクチベーション手順の間に、GGSNは、PDPコンテクストを指すのに使用されるべきトンネルエンドポイント識別子を割り当ててもよい。

【0020】

図2は、ゲートウェイサポートノードGGSNにおいて本発明の第1の好ましい実施形態によるオペレーションを示すフローチャートである。本発明の第1の好ましい実施形態では、パケットに含まれたソースアドレスが、その形式がなりすましを可能にするPDPコンテクストのみにおいて、アクチベートされたパケットデータアドレスと比較される。これらは、IP形式のコンテクスト及びパケットデータアドレスを含む。これらの形式（又は1つの形式）は、比較を実行す

るノードにおいて定義される。図2の例では、なりすましが、IPアドレスについてのみ可能であり、他のパケットデータアドレス形式では成功しないと仮定する。又、移動ステーションは、それが使用するPDPコンテクスト（即ち、例えばIPアドレスを仮定する）をアクチベートし、そしてIPパケットを、例えば図1に示すサーバー1又はインターネット4に送信すると仮定する。更に、トンネルを識別するのにTIDが使用されると仮定する。

【0021】

図2を参照すれば、ステップ200において、GGSNは、独特のトンネルを使用してパケットを受信し、ステップ201においてそれをカプセル解除し、そしてステップ202においてトンネル識別子TIDを抽出する。ステップ203において、GGSNは、TIDにより、TIDに対応するPDPコンテクストのPDPコンテクスト情報を検索する。この情報は、パケットデータアドレス、この例ではIPアドレスで表わされたPDPアドレスを含む。次いで、ステップ204において、GGSNは、トンネルに対応するPDPコンテクスト（即ちパケットデータアドレス）がIP形式のものであるかどうかチェックする。もしそうであれば、GGSNは、ステップ205において、パケットのタイトルに与えられたソースアドレスを抽出する。GGSNは、両方のアドレスを知ると、それらをステップ206において比較する。ソースアドレスが、PDPコンテクストのPDPアドレスと同じである場合には、移動ステーションは、IPパケットに含まれることを請求し、その結果、GGSNは、ステップ207においてパケットを転送する。ソースアドレスがPDPアドレスと相違する場合には、移動ステーションは、別の移動ステーションを偽称し、それ故、GGSNは、ステップ208においてパケットを拒絶する。ここで、拒絶とは、パケットが行先アドレスに送信されないことを意味する。

【0022】

拒絶の後にパケットに何が起きるかは、オペレータの定義に依存し、本発明には関わりない。例えば、ユーザ及びターミナルは、制御平面シグナリングを使用することにより、ソースアドレスが然るべきものでないことが通知されてもよい。例えば、GGSNは、アラームメッセージをオペレータのネットワークオペレ

ーション及びメンテナンスセンターに送信してもよい。又、PDPコンテクスト情報及びパケット情報を含むエントリーをエラーログファイルへ行うこともできる。又、拒絶されたパケットの内容がエラーログファイルに書き込まれてもよい。更に、ユーザ及びターミナルに偽のソースアドレスであることを通知する更に別の形態は、不正パケットを送信するのに使用されたPDPコンテクストをデアクチベートすることである。PDPコンテクストは、例えば、GGSN、SGSN及びMSにおいてデアクチベートされ、従って、GGSNは、PDPコンテクストをデアクチベートするようにSGSNに要求し（又はパケットを拒絶するのがSGSNである場合にはSGSNがデアクチベーション要求をGGSNに送信し）、そしてSGSNは、PDPコンテクストをデアクチベートするようにMSに要求する。デアクチベーション要求メッセージは、MS又はMSに関連したアプリケーションが偽の又は不正なソースアドレスを使用したことを指示する特定のデアクチベーションコードを原因コードとして含むのが好ましい。この特定の原因コードの結果として、ユーザには、偽のソースアドレスを使用する試みであることが通知される。この通知を使用する主たる理由は、ユーザが不正行為を思いとどまるようにするか、又はユーザに偽のソースアドレスを使用したアプリケーションが通知されることである。エンドユーザへの通知は、偽のソースアドレスでデータを送信しようと試みたアプリケーションを識別するテキストメッセージ又はメッセージウインドウであるのが好ましい。又、上述した動作は、所定量の不正パケットが拒絶された後にのみ実行されてもよい。偽のソースアドレスの使用がMSに通知されると、例えば、GGSNがMS及び／又はオペレータネットワーク及びメンテナンスセンターに送信するメッセージは、偽のソースアドレスを有するパケットの上位層プロトコル（例えば、TCP又はUDP）ヘッダに関するある情報を搬送するのが好ましい。これは、不正のアプリケーション及び不正活動の目的を容易に見出せるようとする。メッセージは、拒絶されたパケットの全内容を含んでもよい。拒絶されたパケットのパケット流は、オペレータのネットワークオペレーション及びメンテナンスセンターのような外部ノードへ転送されてもよい。

ステップ204において、PDPがIP形式でないことが通知された場合に、GGSNは、ステップ207へ直接進み、そしてパケットを転送する。

ステップ206におけるチェックの目的は、誰か別の者を偽っていない送信者のパケットだけがGGSNにより外部ネットワークに転送されるように確保することである。本発明により送信者を認証するには簡単なチェックだけで充分であり、認証シグナリングは必要とされない。

【0024】

本発明の別的好ましい実施形態では、ステップ206のチェックがSGSNにおいて実行され、そしてステップ201が省略される。というのは、移動ステーションから受信されるパケットがカプセル化されないからである。他の好ましい実施形態では、SGSNが、ステップ202において、TIDではなく、MSから受信したパケットからTLLI及びNSAPIを抽出する。TLLIは、ルーティングエリア内でMS、ひいては、IMSIを独特に識別する。NSAPIは、このパケットと共にMSにより使用されるPDPコンテクストを識別する。TLLI及びNSAPIを使用して、SGSNは、PDPコンテクスト情報を検索する。他の好ましい実施形態では、TID（又はPDPコンテクストを識別する他の対応する情報）がパケットに追加され、そしてパケットは、ステップ207の前に、即ちパケットがGGSNに送信される前に、カプセル化される。

【0025】

将来、PDPアドレスのアドレススペースは、1つのPDPコンテクストに関連されるか、或いは対応する接続定義に関連されることになろう。アドレススペースは、例えば、許容PDPアドレスのリストである。この場合に、パケットに含まれるソースアドレスは、この許容アドレス間にあれば充分である。同様に、将来、許容PDPアドレスの一部分を定義することにより、PDPコンテクスト情報は、許容PDPアドレスを1組の許容アドレス（即ちアドレススペース）として指定することができる。この場合に、パケットのソースアドレスは、アドレスの定義された部分を含まねばならず、即ちソースアドレスは、1組の許容アドレスに属していかなければならない。又、アドレススペースは、上述の両方の方法を使用することにより定義されてもよい。アドレススペースは、他の何らかの方

法で定義することもできる。

【0026】

なりすましを可能にする多数のパケットデータアドレス形式が定義される実施形態では、ステップ204において、パケットに使用されるパケットデータアドレスがそれらの1つであるかどうかチェックされる。もしそうであれば、ステップ205から続ける。さもなければ、ステップ207へ進む。

本発明のある好ましい実施形態では、パケットに含まれたソースアドレスは、アクチベートされたパケットデータアドレスの形式には関わりなく、アクチベートされたパケットデータアドレスと比較される。この場合に、ステップ204のチェックは行われず、ステップ206のチェックが各パケットに対して実行される。

【0027】

図2に示すステップの順序は、上述したものとは異なってもよく、又、それらステップは、同時に実行することもできる。例えば、ステップ204は、ステップ201の前に実行することができ、そしてステップ203は、ステップ205と同時に実行することができる。これらのステップ間に、図示されていないステップを実行することもできる。ある実施形態では、ステップ201及び／又は204を省略することもできる。ステップ202では、TIDに代わって、PDPコンテクストを識別する他の情報を抽出することができる。

【0028】

現状技術によるサービスを実施するのに必要な手段に加えて、本発明の機能を実施するテレコミュニケーションシステム、テレコミュニケーションネットワーク及びネットワークノードは、パケットに含まれたアドレスを、パケットの送信者に対してアクチベートされた即ち許容されたアドレス（1つ又は複数）と比較するための手段を備えている。既存のネットワークノードは、本発明による機能に使用できるプロセッサ及びメモリを備えている。本発明を実施するのに必要な全ての変更は、付加的な又は更新されたソフトウェアルーチンとして及び／又はアプリケーション回路（ASIC）により実施することができる。

ネットワークのエッジ要素（SGSN又はGGSN）が加入者を認証すること

を上記で説明したが、本発明は、エッジ要素に限定されるものではない。比較に必要なアドレス情報が記憶される別のネットワークノードが比較を実行することもできる。

【0029】

上記の「パケットデータプロトコルPDP」又は「PDPコンテクスト」という語は、一般に、ターミナル（例えば移動ステーション）の状態及び少なくとも1つのネットワーク要素又は機能を指すものと理解されたい。この状態は、ターミナルにより使用されるネットワーク（例えば移動通信ネットワーク）を経て、データパケットに対する特定数のパラメータを有する送信経路、即ちトンネルを生じさせる。又、ここで使用する「ノード」という語は、PDPトンネルを経て送信されるデータパケットを処理するネットワーク要素又は機能を一般的に指す用語であると解釈されたい。

上記説明及び添付図面は、本発明を単に例示するものに過ぎないことを理解されたい。特許請求の範囲に規定された本発明の精神及び範囲から逸脱せずに種々の変更がなされ得ることが当業者に明らかであろう。

【図面の簡単な説明】

【図1】

GPRSサービスのネットワークアーキテクチャーを示すブロック図である。

【図2】

本発明による動作を示すフローチャートである。

【図1】

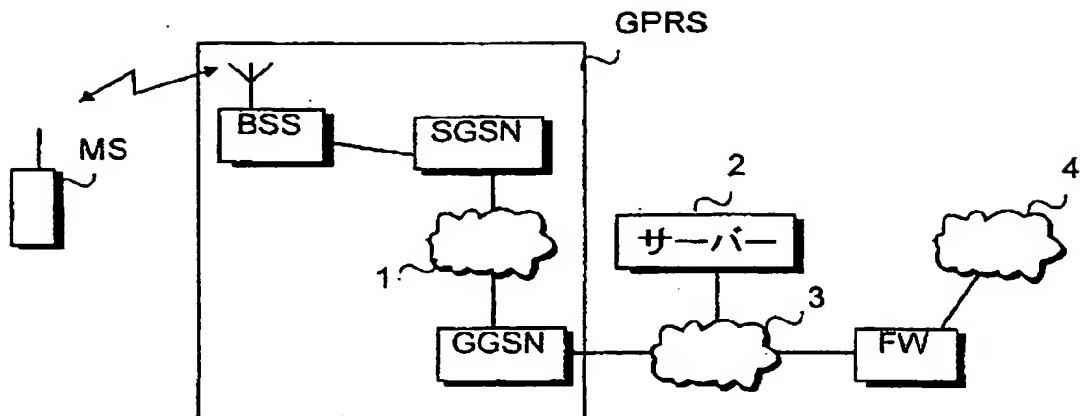


FIG.1

【図2】

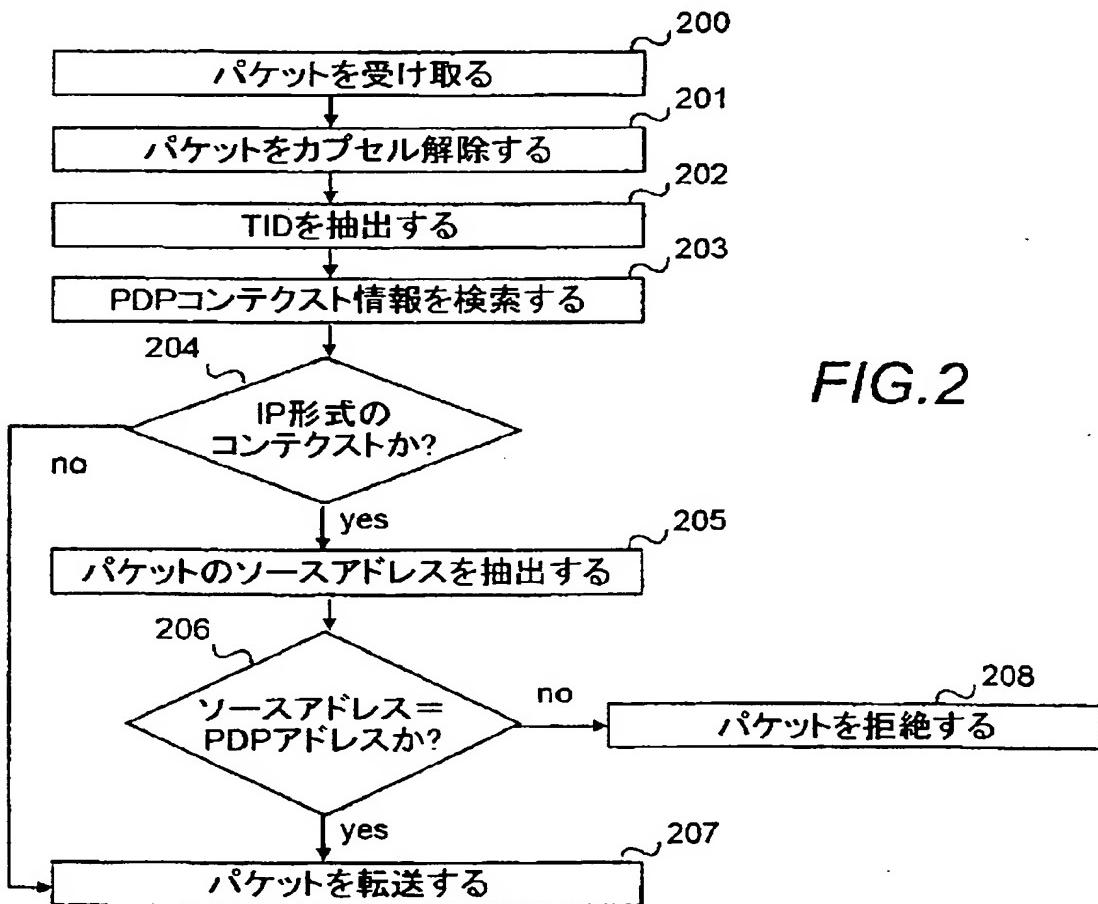


FIG.2

【国际調査報告】

INTERNATIONAL SEARCH REPORT		International application No. PCT/FI 00/01114
A. CLASSIFICATION OF SUBJECT MATTER		
IPC7: H04L 9/32, H04L 12/00, H04L 12/28 According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols)		
IPC7: H04L, H04Q, G06F		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
SE, DK, FI, NO classes as above		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category ^a	Character of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 9948303 A2 (CISCO TECHNOLOGY, INC.), 23 Sept 1999 (23.09.99), page 4, line 26 - page 7, line 20, figures 2,3, claims 1-14, abstract --	1-12
Y	WO 9917499 A2 (NOKIA TELECOMMUNICATIONS OY), 8 April 1999 (08.04.99), page 8, line 6 - line 29, figure 3, claims 1-20, abstract --	1-12
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubt on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed		
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "G" document member of the same patent family		
Date of the actual completion of the international search 23 March 2001	Date of mailing of the international search report 30-03-2001	
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Klas Arvidsson/JAN Telephone No. +46 8 782 25 00	

INTERNATIONAL SEARCH REPORT

International application No. PCT/FI 00/01114
--

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Description of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>1997 IEEE Symposium on Proceedings, Security and Privacy. "Analysis of a denial of service attack on TCP" Schuba, C.L., et al Page 210, column 2, line 25 - page 211, column 1, line 52; page 214, column 2, line 19 - page 217, col umn 2, line 9. Figures 8,9,11</p> <p>---</p> <p>-----</p>	1-12

INTERNATIONAL SEARCH REPORT
Information on patent family membersInternational application No.
PCT/FI 00/01114

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
WO 9948303 A2	23/09/99	AU	3098295 A	11/10/99
WO 9917499 A2	08/04/99	AU CN EP FI	9351598 A 1277771 T 1018241 A 973806 A	23/04/99 20/12/00 12/07/00 27/03/99

フロントページの続き

(81) 指定国 EP(AT, BE, CH, CY,
DE, DK, ES, FI, FR, GB, GR, IE, I
T, LU, MC, NL, PT, SE, TR), OA(BF
, BJ, CF, CG, CI, CM, GA, GN, GW,
ML, MR, NE, SN, TD, TG), AP(GH, G
M, KE, LS, MW, MZ, SD, SL, SZ, TZ
, UG, ZW), EA(AM, AZ, BY, KG, KZ,
MD, RU, TJ, TM), AE, AG, AL, AM,
AT, AU, AZ, BA, BB, BG, BR, BY, B
Z, CA, CH, CN, CR, CU, CZ, DE, DK
, DM, DZ, EE, ES, FI, GB, GD, GE,
GH, GM, HR, HU, ID, IL, IN, IS, J
P, KE, KG, KP, KR, KZ, LC, LK, LR
, LS, LT, LU, LV, MA, MD, MG, MK,
MN, MW, MX, MZ, NO, NZ, PL, PT, R
O, RU, SD, SE, SG, SI, SK, SL, TJ
, TM, TR, TT, TZ, UA, UG, US, UZ,
VN, YU, ZA, ZW

Fターム(参考) 5K030 GA15 HA08 HC01 HC09 HD03

KA05 LB05 LC15

5K067 AA30 BB21 DD17 GG01 GG11

HH05 HH22 HH24